

## SELF-DUAL CODES OVER $\mathbb{Z}_{p^2}$ OF SMALL LENGTHS

WHAN-HYUK CHOI AND YOUNG HO PARK<sup>†,\*</sup>

ABSTRACT. Self-dual codes of lengths less than 5 over  $\mathbb{Z}_p$  are completely classified by the second author [The classification of self-dual modular codes, *Finite Fields Appl.* **17** (2011), 442-460]. The number of such self-dual codes are also determined. In this article we will extend the results to classify self-dual codes over  $\mathbb{Z}_{p^2}$  of length less than 5 and give the number of codes in each class. Explicit and complete classifications for small  $p$ 's are also given.

### 1. Introduction

A code over  $\mathbb{Z}_{p^e}$  of length  $n$  is a  $\mathbb{Z}_{p^e}$ -submodule of  $\mathbb{Z}_{p^e}^n$ . Codes of length  $n$  over  $\mathbb{Z}_{p^e}$  have generator matrices permutation equivalent to the *standard form*

$$(1) \quad G = \begin{pmatrix} I_{k_0} & A_{01} & A_{02} & A_{03} & \cdots & A_{0,e-1} & A_{0e} \\ 0 & pI_{k_1} & pA_{12} & pA_{13} & \cdots & pA_{1,e-1} & pA_{1e} \\ 0 & 0 & p^2I_{k_2} & p^2A_{23} & \cdots & p^2A_{2,e-1} & p^2A_{2e} \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & p^{e-1}I_{k_{e-1}} & p^{e-1}A_{e-1,e} \end{pmatrix},$$

where the columns are grouped into blocks of sizes  $k_0, k_1, \dots, k_e$ , and the  $k_i$  are nonnegative integers adding to  $n$  [4]. A matrix with this standard

---

Received August 9, 2017. Revised August 30, 2017. Accepted September 13, 2017.

2010 Mathematics Subject Classification: 11T71, 94B60.

Key words and phrases: self-dual code, modular codes.

<sup>†</sup> This research is supported by 2015 Research Grant from Kangwon National University (No. 520150414).

\* Corresponding author.

© The Kangwon-Kyungki Mathematical Society, 2017.

This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution and reproduction in any medium, provided the original work is properly cited.

form is said to be of *type*

$$(2) \quad (1)^{k_0}(p)^{k_1}(p^2)^{k_2} \dots (p^{e-1})^{k_{e-1}}.$$

The number of nonzero rows is called the *rank* of  $M$  and denoted by  $\text{rank } M$ .  $k_0$  is called the *free rank*.

The ambient space  $\mathbb{Z}_{p^e}^n$  is endowed with the standard inner product

$$(v_1, \dots, v_n) \cdot (w_1, \dots, w_n) = v_1w_1 + \dots + v_nw_n.$$

For a code  $C$  of length  $n$  over  $\mathbb{Z}_{p^e}$ , the dual code  $C^\perp$  of  $C$  is defined by

$$C^\perp = \{\mathbf{v} \in \mathbb{Z}_{p^e}^n \mid \mathbf{v} \cdot \mathbf{w} = 0 \text{ for all } \mathbf{w} \in C\}.$$

If  $C$  is a code of length  $n$  over  $\mathbb{Z}_{p^e}$  with generator matrix of the form (1) then  $C^\perp$  has generator matrix of the form

$$G^\perp = \begin{pmatrix} B_{0e} & B_{0,e-1} & \dots & B_{03} & B_{02} & B_{01} & I_{k_e} \\ pB_{1e} & pB_{1,e-1} & \dots & pB_{13} & pB_{12} & pI_{k_{e-1}} & 0 \\ p^2B_{2e} & p^2B_{2,e-1} & \dots & p^2B_{23} & p^2I_{k_{e-2}} & 0 & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ p^{e-1}B_{e-1,e} & p^{e-1}I_{k_1} & \dots & 0 & 0 & 0 & 0 \end{pmatrix}$$

where the column blocks have the same size as in  $G$  [4]. If  $C$  has type  $1^{k_0}(p)^{k_1} \dots (p^{e-1})^{k_{e-1}}$  then the dual code has type  $1^{k_e}p^{k_{e-1}}(p^2)^{k_{e-2}} \dots (p^{e-1})^{k_1}$ , where  $k_e = n - \sum_{i=0}^{e-1} k_i$ .

$C$  is *self-orthogonal* if  $C \subset C^\perp$ .  $C$  is *self-dual* if  $C = C^\perp$ . If  $C$  is self-dual with type  $1^{k_0}(p)^{k_1} \dots (p^{e-1})^{k_{e-1}}$ , then  $k_i = k_{e-i}$  for all  $i$ . For any code  $C$  of length  $n$  over  $\mathbb{Z}_{p^e}$   $|C||C^\perp| = p^{en}$ . If  $C$  is a self-orthogonal code of length  $n$  and  $|C| = p^{en/2}$ , then  $C$  is self-dual.

Next we discuss the equivalence of self-dual codes. Let

$$\mathbb{D} = \mathbb{D}_m^n = \{\text{diag}(\gamma_1, \gamma_2, \dots, \gamma_n) \mid \gamma_i \in \mathbb{Z}_m, \gamma_i^2 = 1\}.$$

and let  $\mathbb{T}_m = \mathbb{T}_m^n$  be the group of all *monomial transformations* on  $\mathbb{Z}_m^n$  defined by

$$\mathbb{T}_m = \{\gamma\sigma \mid \gamma \in \mathbb{D}, \sigma \in S_n\}$$

as in [8]. We will use the same notations and terminology as in [8]. The group  $\mathbb{T}_m$  acts on the set of all self-dual codes of length  $n$  over  $\mathbb{Z}_m$  by  $Ct = \{ct \mid c \in C\}$ . Two self-dual codes  $C$  and  $C'$  are *equivalent* (denoted  $C \sim C'$ ) if there exists an element  $t \in \mathbb{T}_m^n$  such that  $Ct = C'$ . The group of all automorphisms of  $C$  will be denoted by  $\text{Aut}(C)$ .

Self-dual codes of lengths less than 5 over  $\mathbb{Z}_p$  are completely classified in [8]. The number of such self-dual codes are also determined. In this article we will classify self-dual codes over  $\mathbb{Z}_{p^2}$  of length less than 5.

### 2. Self-dual codes over $\mathbb{Z}_{p^2}$

For codes over  $\mathbb{Z}_{p^2}$ , every code  $C$  over  $\mathbb{Z}_{p^2}$  is permutation equivalent to a code with generator matrix in standard form:

$$G = \begin{pmatrix} I_{k_1} & A_1 & B_1 + pB_2 \\ 0 & pI_{k_2} & pC_1 \end{pmatrix}$$

where  $A_1, B_1, B_2, C_1$  are matrices with entries from  $\{0, 1, \dots, p - 1\}$ . Associated with  $C$  there are two codes over  $\mathbb{Z}_p$ , the *residue code*

$$R(C) = \{x \in \mathbb{Z}_p^n : \exists y \in \mathbb{Z}_p^n \text{ such that } x + py \in C\}$$

and the *torsion code*  $\text{Tor}(C) = \{y \in \mathbb{Z}_p^n : py \in C\}$  which have generator matrices

$$R(C) = (I_{k_1} \ A_1 \ B_1), \quad \text{Tor}(C) = \begin{pmatrix} I_{k_1} & A_1 & B_1 \\ 0 & I_{k_2} & C_1 \end{pmatrix}$$

respectively. If  $C$  is self-dual, then  $R(C)$  is self-orthogonal.

**THEOREM 2.1.** *Let  $p$  be an odd prime. There is a one-one correspondence between self-dual codes  $C$  of free rank 1 over  $\mathbb{Z}_{p^2}$*

$$C : \begin{pmatrix} 1 & a_2 & a_3 & \dots & a_{n-1} & a_n + pb_1 \\ & p & & & & pb_2 \\ & & p & & & pb_3 \\ & & & \ddots & & \vdots \\ & & & & p & pb_{n-1} \end{pmatrix}$$

where  $n$  is the length of the code,  $0 \leq a_i, b_j < p$ , and self-orthogonal codes  $R(C) = (1 \ a_2 \ \dots \ a_{n-1} \ a_n)$  over  $\mathbb{Z}_p$ .

**THEOREM 2.2.** *If  $C$  is a self-dual code of free rank 1 over  $\mathbb{Z}_{p^2}$ , then  $\text{Aut}(C) = \text{Aut}(R(C))$ .*

**THEOREM 2.3.** [9] *Let  $\sigma_p(n, k)$  be the number of self-orthogonal codes of length  $n$  and dimension  $k$  over  $\mathbb{Z}_p$ , where  $p$  is odd prime. Then*

1. *If  $n$  is odd,*

$$\sigma_p(n, k) = \frac{\prod_{i=0}^{k-1} (p^{(n-1-2i)} - 1)}{\prod_{i=1}^k (p^i - 1)}.$$

2. If  $n$  is even and  $k \geq 2$ ,

$$\sigma_p(n, k) = \frac{(p^{n-k} + \eta((-1)^{\frac{n}{2}})(p^k - 1)p^{\frac{n}{2}-k}) \prod_{i=1}^{k-1} (p^{n-2i} - 1)}{\prod_{i=1}^k (p^i - 1)}.$$

Here  $\eta$  is the quadratic character of  $\mathbb{Z}_p$ .

**THEOREM 2.4.** [1] *Let  $p$  be an odd prime. Given a self-orthogonal code  $C_p$  of dimension  $k$  over  $\mathbb{Z}_p$ , there are  $p^{k(k-1)/2}$  self-dual codes over  $\mathbb{Z}_{p^2}$  whose residue code is  $C_p$ . Therefore, the number of self-dual codes of length  $n$  over  $\mathbb{Z}_{p^2}$  is  $N_{p^2}(n) = \sum_{0 \leq k \leq \lfloor n/2 \rfloor} \sigma_p(n, k) p^{k(k-1)/2}$ .*

**THEOREM 2.5.** *If  $n$  is even,  $\sigma_p(n, 1) = \frac{p^{n-1} + \eta((-1)^{\frac{n}{2}})(p-1)p^{\frac{n}{2}-1}}{p-1}$ .*

*Proof.* The number of solutions of  $x_1^2 + \dots + x_n^2 = 0$  in  $\mathbb{Z}_p$  is given by  $p^{n-1} + \eta((-1)^{n/2})(p-1)p^{\frac{n}{2}-1}$  [5]. □

### 3. Classification

There is a unique self-dual codes ( $p$ ) of length 1 over  $\mathbb{Z}_{p^2}$  and there is a (unique) inequivalent self-dual code  $(1 \ a)$  over  $\mathbb{Z}_{p^2}$  of length 2 if and only if  $p \equiv 1 \pmod{4}$ . It is clear that  $\begin{pmatrix} p & \\ & p \end{pmatrix}$  is a self-dual code over  $\mathbb{Z}_{p^2}$ .

The types of self-dual codes of length 3 are  $1^{e_0} p^{e_1}$ , where  $2e_0 + e_1 = 3$ . Thus any self-dual code  $C$  of length 3 over  $\mathbb{Z}_{p^2}$  is equivalent to

$$\begin{pmatrix} p & & \\ & p & \\ & & p \end{pmatrix} \text{ or } C_{a,b} : \begin{pmatrix} 1 & a & b+pb_1 \\ & p & pc \end{pmatrix}$$

where  $0 \leq a, b, b_1 < p$  and  $b \neq 0$ .

For binary case,  $(2) \oplus (2) \oplus (2)$  is the only self-dual code over  $\mathbb{Z}_4$  of length 3, and for ternary case there are two classes of self-dual codes over  $\mathbb{Z}_9$  of length 3:

$$(3) \oplus (3) \oplus (3), \quad \begin{pmatrix} 1 & 2 & 2 \\ & 3 & 6 \end{pmatrix}.$$

**THEOREM 3.1.** *Let  $p \neq 2, 3$ . Then the non-trivial self-dual code over  $\mathbb{Z}_{p^2}$  of length 3 is equivalent to one of the following classes of inequivalent codes:*

Class	$C_{a,b}$	$\text{Aut}(C_{a,b})$
(i)	$a = 0$	$4.\{(1), (13)\}$
(ii)	$a^6 = 1, a \neq \pm 1$	$2.\{(123)\}$
(iii)	$a^2 = 1, b^2 + 2 = 0$	$2.\{(12)\}$
(iv)	else	$2.(1)$

**THEOREM 3.2.** *For  $p \neq 2, 3$ , let  $N_1, N_2, N_3, N_4$  be the number of class (i), (ii), (iii), (iv) self-dual codes over  $\mathbb{Z}_{p^2}$  of length 3, respectively. These numbers are determined as follows.*

$p \pmod{24}$	$N_1$	$N_2$	$N_3$	$N_4$
1	1	1	1	$\frac{p-25}{24}$
5	1	0	0	$\frac{p-5}{24}$
7	0	1	0	$\frac{p-7}{24}$
11	0	0	1	$\frac{p-11}{24}$
13	1	1	0	$\frac{p-13}{24}$
17	1	0	1	$\frac{p-17}{24}$
19	0	1	1	$\frac{p-19}{24}$
23	0	0	0	$\frac{p+1}{24}$

*Proof.* We have the one-to-one correspondence between the set of self-dual codes over  $\mathbb{Z}_p$ , the set of self-orthogonal codes over  $\mathbb{Z}_{p^2}$  and the set of self-dual codes over  $\mathbb{Z}_{p^2}$  as follows:

$$\begin{pmatrix} 1 & a & b \\ & 1 & -b \\ & & a \end{pmatrix} \leftrightarrow (1 \ a \ b) \leftrightarrow \begin{pmatrix} 1 & a & b + pb_1 \\ & p & pc \end{pmatrix}$$

where  $1 + a^2 + b^2 = 0 \pmod{p}$ . □

For  $5 \leq p \leq 67$ , we give the classification in the following table. Here  $(a, b)$  denotes the code  $C_{a,b}$ .

$p^2$	(i)	(ii)	(iii)	(iv)
$5^2$	(0,7)			
$7^2$		(2,32)		
$11^2$			(1,19)	
$13^2$	(0,70)	(3,126)		
$17^2$	(0,38)		(1,24)	
$19^2$		(7,315)	(1,63)	
$23^2$				(2,169)
$29^2$	(0,41)			(2,71)
$31^2$		(5,800)		(4,142)
$37^2$	(0,117)	(10,248)		(3,510)
$41^2$	(0,378)		(1,71)	(2,703)
$43^2$		(36,49)	(1,801)	(2,826)
$47^2$				(2,1052), (3,361)
$53^2$	(0,500)			(3,231), (4,1172)
$59^2$			(1,1275)	(3,1246), (6,776)
$61^2$	(0,682)	(13,1328)		(2,774), (8,1259)
$67^2$		(29,1645)	(1,2030)	(2,2091), (12,1626)

Next, we consider the codes of length 4. The types of self-dual codes of length 4 are  $1^{e_0}p^{e_1}$ , where  $2e_0 + e_1 = 4$ . Thus any self-dual code  $C$  of length 4 over  $\mathbb{Z}_{p^2}$  is equivalent to one of

1.  $(p)^4$ ,
2.  $C_{a,b}^2 : \begin{pmatrix} 1 & a & b \\ & 1 & -b \\ & & a \end{pmatrix}$
3.  $C_{a,b,c}^1 : \begin{pmatrix} 1 & a & b & c+pc_1 \\ & p & p & pc_2 \\ & & p & pc_3 \end{pmatrix}$  where  $0 \leq a, b, c < p$  and  $c \neq 0$ .

There are two classes of self-dual codes over  $\mathbb{Z}_4$  of length 4:

$$(2) \oplus (2) \oplus (2) \oplus (2), \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ & 2 & & \\ & & 2 & \\ & & & 2 \end{pmatrix}$$

and there are three classes of self-dual codes over  $\mathbb{Z}_9$  of length 4:

$$(3) \oplus (3) \oplus (3), \quad \begin{pmatrix} 1 & 1 & 4 \\ & 1 & 5 \\ & & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 4 \\ & 3 & 3 \\ & & 6 \end{pmatrix}$$

**THEOREM 3.3.** *Let  $p \neq 2, 3$ . Then the self-dual code*

$$C_{a,b}^2 : \begin{pmatrix} 1 & a & b \\ & 1 & -b \\ & & a \end{pmatrix}$$

*over  $\mathbb{Z}_{p^2}$  is one of the following four classes of inequivalent codes:*

Class	$C_{a,b}^2$	$\text{Aut}(C_{a,b}^2)$
(i)	$a^2 + 1 = 0, b = 0$	$4.B_8$
(ii)	$a^6 = 1, a \neq \pm 1$	$2.A_4$
(iii)	$a^2 = 1, b^2 + 2 = 0$	$2.B_8$
(iv)	else	$2.B_4$

*Codes from classes (i),(ii),(iii) are unique, if exist, up to equivalence.*

**THEOREM 3.4.** *For  $p \neq 2, 3$ , let  $N_1, N_2, N_3, N_4$  be the number of class (i), (iii), (iv) self-dual codes over  $\mathbb{Z}_{p^2}$  of length 4 and free rank 2, respectively. These numbers are determined as follows.*

$p \pmod{24}$	$N_1$	$N_2$	$N_3$	$N_4$
1	1	1	1	$\frac{p^2+p-26}{24}$
5	1	0	0	$\frac{p^2+p-6}{24}$
7	0	1	0	$\frac{p^2+p-8}{24}$
11	0	0	1	$\frac{p^2+p-12}{24}$
13	1	1	0	$\frac{p^2+p-14}{24}$
17	1	0	1	$\frac{p^2+p-18}{24}$
19	0	1	1	$\frac{p^2+p-20}{24}$
23	0	0	0	$\frac{p^2+p}{24}$

*Proof.* The number of self-dual codes over  $\mathbb{Z}_{p^2}$  of length 4 and free rank 2 is given by  $\sigma_p(4, 2)p = 2(p + 1)p$ . By the mass formula

$$N_4 = \frac{1}{48}(2(p + 1)p - 12N_1 - 16N_2 - 24N_3).$$

Here  $48 = \frac{2^4 \cdot 4!}{|2.B_4|}$ ,  $12 = \frac{2^4 \cdot 4!}{|4.B_8|}$ , etc. □

**THEOREM 3.5.** *Let  $p \neq 2, 3$ . Then any self-dual code  $C_{a,b,c}^1$  of rank 3 is equivalent to one of the following inequivalent codes:*

Class	$C_{a,b,c}^1$	$\text{Aut}(C_{a,b,c}^1)$
(i)	$a = b = 0$	$8.\langle(14), (23)\rangle$
(ii)	$b = 0, a^6 = 1, a^2 \neq 1, c^2 \neq 1$	$4.\langle(124)\rangle$
(iii)	$b = 0, a^2 = 1$	$4.S_2$
(iv)	$b = 0, a \neq 0, a^6 \neq 1, c^6 \neq 1, a^2 \neq c^2$	$4.(1)$
(v)	$a^2 = 1 \neq b^2 = c^2$	$2.\langle(1324), (12)\rangle$
(vi)	$a^2 = b^2 = 1$	$2.S_3$
(vii)	$1 = a^2, b^2, c^2$ distinct	$2.S_2$
(viii)	$a^2 = -1, b^2 \neq \pm 1, b^4 \neq -1$	$2.\{(1), (14)(23)\}$
(ix)	$a^2 = -1, b^2 \neq \pm 1, b^4 = -1$	$2.\langle(1243)\rangle$
(x)	$1, a^2, b^2, c^2$ are all distinct, $a^2, b^2, c^2 \neq -1$	$2.(1)$

*Proof.* It is enough to classify  $R(C) = \langle(1, a, b, c)\rangle$  over  $\mathbb{Z}_p$ . When  $b = 0$ , the classification goes back to the case of  $C_{a,c}^2$ . Suppose  $b \neq 0$ . For  $t = \gamma\sigma \in \mathbb{T}$ ,  $\sigma \in S_4$ ,  $k \in \mathbb{Z}_p$ , we have that

$$(1, a, b, c)\gamma\sigma = k(1, a, b, c) \iff (1, a^2, b^2, c^2)\sigma = k^2(1, a^2, b^2, c^2).$$

Thus  $k^2 = 1, a^2, b^2, c^2$  and  $\sigma$  can be determined once we know the equalities among  $1, a^2, b^2, c^2$ . For example, suppose that  $1 = a^2, b^2, c^2$  are distinct. Now  $(1, 1, b^2, c^2)\sigma = (k^2, k^2, k^2b^2, k^2c^2)$  implies that  $k^2 = 1, \sigma(1) = 1, 2$  and  $\sigma(3) = 3, \sigma(4) = 4$ . Next, for  $\gamma \in \mathbb{D}$ ,  $(1, 1, b, c)\gamma = k(1, 1, b, c)$  implies  $\gamma = \pm(1, 1, 1, 1)$ . □

**THEOREM 3.6.** *For  $p \neq 2, 3$ , let  $N_1, N_2, \dots, N_{10}$  be the number of class (i), (ii),  $\dots$ , (x) self-dual codes over  $\mathbb{Z}_{p^2}$  of length 4 and free rank 1, respectively. These numbers are determined as follows.*

$p$ (24)	$N_1$	$N_2$	$N_3$	$N_4$	$N_5$	$N_6$	$N_7$	$N_8$	$N_9$	$N_{10}$
1	1	1	1	$\frac{p-25}{24}$	1	1	$\frac{p-17}{8}$	$\frac{p-9}{8}$	1	$\frac{(p+1)^2-28p+216}{192}$
5	1	0	0	$\frac{p-5}{24}$	1	0	$\frac{p-5}{8}$	$\frac{p-5}{8}$	0	$\frac{(p+1)^2-28p+104}{192}$
7	0	1	0	$\frac{p-7}{24}$	0	1	$\frac{p-7}{8}$	0	0	$\frac{(p+1)^2-16p+48}{192}$
11	0	0	1	$\frac{p-11}{24}$	0	0	$\frac{p-3}{8}$	0	0	$\frac{(p+1)^2-16p+32}{192}$
13	1	1	0	$\frac{p-13}{24}$	1	1	$\frac{p-13}{8}$	$\frac{p-5}{8}$	0	$\frac{(p+1)^2-28p+168}{192}$
17	1	0	1	$\frac{p-17}{24}$	1	0	$\frac{p-9}{8}$	$\frac{p-9}{8}$	1	$\frac{(p+1)^2-28p+152}{192}$
19	0	1	1	$\frac{p-19}{24}$	0	1	$\frac{p-11}{8}$	0	0	$\frac{(p+1)^2-16p+96}{192}$
23	0	0	0	$\frac{p+1}{24}$	0	0	$\frac{p+1}{8}$	0	0	$\frac{(p+1)^2-16p-16}{192}$

*Proof.* We consider the classes (viii) and (ix). In these cases  $\{1, a^2, b^2, c^2\} = \{1, -1, b^2, -b^2\}$ , where  $b^2 \neq 0, \pm 1$ ,  $p \equiv 1 \pmod{4}$ . There exists  $b$  with  $b^4 = -1$  if and only if  $p \equiv 1 \pmod{8}$ , and in that case,  $(1, a, b, c) = (1, i, \pm b, \pm ib)$  or  $(1, i, \pm bi, \pm b)$  with  $i^2 = -1$ , and hence  $N_9 = 1$ .

Now  $(1, a^2, b^2, c^2) \sim (1, -1, \pm b^2, \mp b^2) \sim (1, -1, \pm 1/b^2, \mp 1/b^2)$ . These four are distinct iff  $b^4 \neq -1$ . Thus  $4N_8 + 2N_9 = \frac{(p-1)}{2} - 2$ .

Once  $N_1, \dots, N_9$  is determined,  $N_{10}$  can be computed by the mass formula:

$$\sum_i \frac{2^4 \cdot 4!}{|\text{Aut}(C_i)|} = 3p^2 + 4p + 2,$$

where  $C_i$  runs through the representatives of inequivalent self-dual codes. □

Finally we give the complete classification for small  $p$ 's in the following table. Here  $(a, b, c)$  denotes the codes  $C_{a,b,c}^1$ .

$p^2$	i	ii	iii	iv	v
$5^2$	(0, 0, 7)				(1, 2, 12)
$7^2$		(2, 0, 17)			
$11^2$			(1, 0, 19)		
$13^2$	(0, 0, 70)	(3, 0, 43)			(1, 5, 34)
$17^2$	(0, 0, 38)		(1, 0, 24)		(1, 4, 72)
$19^2$		(7, 0, 46)	(1, 0, 63)		
$23^2$				(2, 0, 169)	
$29^2$	(0, 0, 41)			(2, 0, 71)	(1, 12, 70)
$31^2$		(5, 0, 161)		(4, 0, 142)	
$37^2$	(0, 0, 117)	(10, 0, 248)		(3, 0, 510)	(1, 6, 228)

$p^2$	vi	vii	viii	ix	x
$5^2$					
$7^2$	(1, 1, 12)				
$11^2$		(1, 2, 29)			
$13^2$	(1, 1, 45)		(5, 6, 48)		
$17^2$		(1, 6, 110)	(4, 5, 139)	(4, 8, 53)	
$19^2$	(1, 1, 137)	(1, 5, 50)			(2, 3, 104)
$23^2$		(1, 3, 239) (1, 6, 56) (1, 7, 100)			(2, 4, 212)
$29^2$		(1, 2, 136) (1, 6, 181) (1, 11, 333)	(12, 13, 47) (12, 14, 325) (12, 19, 149)		(3, 5, 96)
$31^2$	(1, 1, 82)	(1, 2, 98) (1, 3, 446) (1, 9, 107)			(2, 44, 234) (2, 9, 289) (3, 8, 53)
$37^2$	(1, 1, 206)	(1, 3, 64) (1, 5, 618) (1, 9, 425)	(6, 7, 143) (6, 8, 248) (6, 9, 609) (6, 12, 298)		(2, 5, 231) (2, 13, 97) (3, 4, 495)

*Remark.* Many of the results in this article reappear in [3] with more details.

## References

- [1] J.M.P. Balmaceda, R.A.L. Betty and F.R. Nemenzo, *Mass formula for self-dual codes over  $\mathbb{Z}_{p^2}$* , Discrete Math. **308** (2009), 2984–3002
- [2] K. Betsumiya, S. Georgiou, T.A. Gulliver, M. Harada, and C. Kououvinos, *On self-dual codes over some prime fields*, Discrete Math. **262** (2009), 37–58.
- [3] W. Choi, *The classification of self-dual codes over Galois rings of length 4*, Ph.D thesis, Kangwon National University, 2017.
- [4] J.H. Conway and N.J.A. Sloane, *Self-dual codes over the integers modulo 4*, J. Comin. Theory Ser. A **62** (1993), 30–45.
- [5] R. Lidl and H. Neiderreiter, "Finite fields" in Encyclop. Math. Its Applic. vol. 20. 2nd ed., Cambridge University Press, Cambridge, 1997
- [6] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.
- [7] G. Nebe, E. Rains and N.J.A. Sloane, *Self-dual codes and invariant theory*, Springer-Verlag, 2006
- [8] Y. H. Park, *The classification of self-dual modular codes*, Finite Fields Appl. **17** (2011), 442-460
- [9] V.S. Pless, *The number of isotropic subspaces in a finite geometry*, Atti. Accad. Naz. Lincei Rend. **39** (1965) 418–421

- [10] V.S. Pless, *On the uniqueness of the Golay codes*, J. Combin. Theory **5** (1968) 215–228
- [11] E. Rains and N.J.A. Sloane, *Self-dual codes*, in the Handbook of Coding Theory, V.S. Pless and W.C. Huffman, eds., Elsevier, Amsterdam, 1998, 177-294.

**Whan-hyuk Choi**

Department of Mathematics  
Kangwon National University  
Chuncheon, Korea  
*E-mail*: whchoi@kangwon.ac.kr

**Young Ho Park**

Department of Mathematics  
Kangwon National University  
Chuncheon, Korea  
*E-mail*: yhpark@kangwon.ac.kr